UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/550,216	09/22/2005	Kei Karasawa	277747US90PCT	1366

22850   7590   07/11/2008
OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER
LAFORGIA, CHRISTIAN A

ART UNIT	PAPER NUMBER
2139	

NOTIFICATION DATE	DELIVERY MODE
07/11/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 February 2008*.
2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.
   4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) *1-18* is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☒ The drawing(s) filed on *22 September 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.
   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a)☒ All   b)☐ Some * c)☐ None of:
      1.☐ Certified copies of the priority documents have been received.
      2.☐ Certified copies of the priority documents have been received in Application No. _____.
      3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
   Paper No(s)/Mail Date *4/11/08; 2/6/08*.

4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1.   The amendment of 19 February 2008 has been noted and made of record.

2.   Claims 1-18 have been presented for examination.

Response to Arguments

3.   Applicant's arguments, see page 10, filed 19 February 2008, with respect to the 35 U.S.C.

101 rejection of claim 7 have been fully considered and are persuasive. The 35 U.S.C. 101

rejection of claim 7 has been withdrawn.

4.   Applicant's arguments, see pages 10 and 11, filed 19 February 2008, with respect to the

35 U.S.C. 101 rejection of claim 18 have been fully considered and are persuasive. The 35

U.S.C. 101 rejection of claim 18 has been withdrawn.

5.   Applicant's arguments, see page 11, filed 19 February 2008, with respect to the 35 U.S.C.

112, 2nd paragraph rejections have been fully considered and are persuasive. The 35 U.S.C. 112,

2nd paragraph rejection of claims 1-18 has been withdrawn.

6.   Applicant's arguments with respect to the prior art rejections filed 19 February 2008 have

been fully considered but they are not persuasive.

7.   In response to applicant's arguments against the references individually, one cannot show

nonobviousness by attacking references individually where the rejections are based on

combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re

Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

8.   The Applicant argues on page 13 of the response filed 19 February 2008 that the cable

network disclosed in Candelore is different from the claimed Internet. The Examiner disagrees.

Candelore discloses in claims 4, 9, 15, 19, 27, 41, 48, 52, and 58 that the data transmitted over

the network may follow the Internet Protocol. One of ordinary skill in the art would realize that

the video data can be transmitted over the Internet, especially since Candelore discloses that the

data may be transmitted via use of the internet protocol. Since Candelore discloses the use of the

Internet Protocol and therefore the rejection is maintained.

9.   Applicant's arguments with regards to the prior art rejections amount to a general

allegation that the claims define a patentable invention without specifically pointing out how the

language of the claims patentably distinguishes them from the references. The Applicant's

arguments merely state that the claim limitations are not the same as the cited prior art without

going into any analysis as to how the claim language is different or how the Examiner's

interpretation of the prior art differs from the invention of the instant application.

10.   See further rejections set forth below.

Information Disclosure Statement

11.   The information disclosure statement (IDS) submitted on 06 February 2008 is in

compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure

statement has been considered by the examiner.

12.   The information disclosure statement filed 11 April 2008 fails to comply with 37 CFR

1.98(a)(1), which requires the following: (1) a list of all patents, publications, applications, or

other information submitted for consideration by the Office; (2) U.S. patents and U.S. patent

application publications listed in a section separately from citations of other documents; (3) the

application number of the application in which the information disclosure statement is being

submitted on each page of the list; (4) a column that provides a blank space next to each

document to be considered, for the examiner's initials; and (5) a heading that clearly indicates

that the list is an information disclosure statement. The information disclosure statement has

been placed in the application file, but the information referred to therein has not been

considered.

Claim Rejections - 35 USC § 103

13.   The text of those sections of Title 35, U.S. Code not included in this action can be found

in a prior Office action.

14.   Claims 1-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent

Application Publication No. 2002/0080827 A1 to Lee, hereinafter Lee, in view of U.S. Patent

No. 2005/0169473 A1 to Candelore, hereinafter Candelore.

15.   As per claims 1 and 13, Lee teaches a packet cryptographic processing proxy apparatus

(Figure 2 [block 100]) connected between the Internet (Figure 2 [block 10]) and a terminal

(Figure 2 [blocks 180, 182, 184, 186, 188]), comprising:

        cryptographic processing part (Figure 2 [block 160]) which performs cryptographic

processing for a received packet which is forwarded from the counterpart apparatus to the

terminal or from the terminal to the counterpart apparatus based on the cryptographic

communication channel information stored in said cryptographic communication channel

information storage part (paragraph 056, i.e. encrypting and decrypting data for the home

appliances).

16.   Lee does not teach a cryptographic communication channel information storage part

which stores cryptographic communication channel information used for establishing a

cryptographic communication channel at least for packet communication on the Internet, in

packet communication between a counterpart apparatus connected to the Internet and the

terminal; a packet determination part which determines from a received packet whether or not to agree with the counterpart apparatus on cryptographic communication channel information for establishing a packet communication channel between the counterpart apparatus and the terminal; a cryptographic communication channel information agreement part which, if the packet determination determines necessity of agreement, makes the agreement and stores the agreed cryptographic communication channel information in said cryptographic communication channel information storage part.

17.   Candelore teaches a gateway (Figure 6 [block 400]) or set-top box (Figures 2 [blocks 36, 136], 3 [blocks 236, 136]) that receives encrypted data from the network or content provider (Figure 7 [block 454]) and processes it with respect to the home appliance (Figures 7 [blocks 458, 462, 466], 8, paragraphs 0032, 0058-0062)

a packet determination part which determines from a received packet whether or not to agree with the counterpart apparatus on cryptographic communication channel information for establishing a packet communication channel between the counterpart apparatus and the terminal (Figure 5 [blocks 370, 374], paragraph 0055);

a cryptographic communication channel information agreement part which, if the packet determination determines necessity of agreement, makes the agreement and stores the agreed cryptographic communication channel information in said cryptographic communication channel information storage part (paragraph 0043, i.e. using entitlement control messages to ensure agreement with the cryptographic protocols).

18.   It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a cryptographic communication channel information storage part which

stores cryptographic communication channel information used for establishing a cryptographic

communication channel at least for packet communication on the Internet, in packet

communication between a counterpart apparatus connected to the Internet and the terminal, a

packet determination part which determines from a received packet whether or not to agree with

the counterpart apparatus on cryptographic communication channel information for establishing

a packet communication channel between the counterpart apparatus and the terminal; a

cryptographic communication channel information agreement part which, if the packet

determination determines necessity of agreement, makes the agreement and stores the agreed

cryptographic communication channel information in said cryptographic communication channel

information storage part, since Candelore states at paragraphs 0032-0034 that it provides a secure

way to transmit signals to a home and provides the home gateway to format the data in

accordance with the appliances specified to use the data.

19.   Regarding claim 2, Lee teaches a filter information storage part which stores sending

source identification information, sending destination identification information, protocol

information indicating a packet communication procedure and processing instruction information

indicating whether or not to perform cryptographic processing, as filter information (Figure 2

[block 130], paragraph 0051, i.e. firewalls function by analyzing the source and destination

information, along with the protocol information); and

        cryptographic processing determination part, which, by referring to said filter information

storage part based on filter information in the packet received by the packet cryptographic

processing apparatus, determining whether or not to perform cryptographic processing of the

received packet by said cryptographic processing means based on the processing instruction

information (Figure 2 [blocks 140, 150], paragraphs 0052-0055).

20.   Regarding claim 3, Candelore teaches a received packet determination part which

determines whether or not a received packet from the counterpart apparatus which is forwarded

to the terminal is valid (Figure 5 [blocks 370, 380], paragraph 0055).

21.   Regarding claim 4, Candelore teaches wherein said cryptographic communication

channel information storage part includes a detachable, tamper-proof device in which at least

part of the cryptographic communication channel information is stored (paragraph 0022, i.e. the

use of a smart card).

22.   Regarding claim 5, Candelore teaches wherein said cryptographic communication

channel information storage part includes a storage medium in which at least part of the

cryptographic communication channel information is changeable (paragraph 0043, i.e. using

entitlement control messages to update descrambling keys and access criteria).

23.   Regarding claim 6, Lee teaches the packet cryptographic processing proxy apparatus

(Figure 2 [block 100]) being logically directly connected to a network interface device of the

terminal (Figure 2 [block 170], paragraph 0057, i.e. wirelessly connected).

24.   Candelore discusses the packet cryptographic processing proxy apparatus (Figures 2 [blocks 36, 136], 3 [blocks 236, 136], 6 [block 400) being logically directly connected to a network interface device of the terminal (Figure 8 [block 530]).

25.   Regarding claim 7, Candelore teaches the packet cryptographic processing proxy apparatus being implemented on a device which is connected between the Internet and the terminal and which has no IP address (Figures 2 [blocks 36, 136], 3 [blocks 236, 136], i.e. set-top boxes do not have IP addresses).

26.   With regards to claim 8, Candelore teaches a terminal information collection part which collects a part of at least one of the cryptographic communication channel information (paragraph 0043, i.e. using entitlement control messages to update descrambling keys and access criteria).

27.   Lee the filter information and stores the information in said filter information storage part (Figure 2 [block 130], paragraph 0051).

28.   Regarding claim 9, Candelore teaches a key information setting part which sets key information for performing cryptographic processing of a packet, in the cryptographic communication channel information agreed by said cryptographic communication channel information agreement part, for the terminal (paragraph 0043, i.e. using entitlement control messages to update descrambling keys and access criteria).

29.   With regards to claim 10, Candelore teaches wherein, if determining necessity of

agreement on cryptographic communication channel information, said packet determination part

determines whether valid cryptographic communication channel information corresponding to

the received packet is stored in said cryptographic communication channel information storage

part, causes said key information setting part to set key information in the cryptographic

communication channel information for the terminal if the valid cryptographic communication

channel information is stored, and causes said cryptographic communication channel information

agreement part to make agreement on cryptographic communication channel information if the

valid cryptographic communication channel is not stored (paragraph 0043, i.e. using entitlement

control messages to update descrambling keys and access criteria).

30.   Concerning claim 11, Candelore teaches wherein, if said packet determination part

determines necessity of agreement on the cryptographic communication channel information,

and address information in the received packet is stored in said filter information storage part,

said packet determination part causes agreement on the key information to be made (paragraph

0043, i.e. using entitlement control messages to update descrambling keys and access criteria).

31.   Concerning claim 12, Lee teaches a terminal information acquisition part which detects

the terminal (Figure 1 [block 170], paragraph 0057), acquires address information from the

terminal and stores the acquired address information in said filter information storage part

(Figure 2 [block 130], paragraph 0051).

32.   Regarding claim 14, Lee teaches referring to a filter information storage part based on filter information in the received packet, determining whether or not to perform cryptographic processing for the received packet (Figure 2 [block 130], paragraph 0051).

33.   Candelore teaches causing the cryptographic processing to be performed if it is determined by the determination that cryptographic processing is to be performed (Figure 5 [blocks 370, 374], paragraph 0055), and causing the received packet to immediately pass or to be discarded if it is determined by the determination that cryptographic processing is not to be performed (Figure 5 [block 380], paragraph 0055).

34.   Regarding claim 15, Candelore teaches setting the agreed cryptographic communication channel information for the terminal (paragraph 0043, i.e. using entitlement control messages to update descrambling keys and access criteria); and

       if agreement is not required, bypassing or discarding the received packet (Figure 5 [block 380], paragraph 0055).

35.   With regards to claim 16, Candelore teaches determining whether valid cryptographic communication channel information corresponding to the received packet is stored in the cryptographic communication channel information storage part (Figure 5 [blocks 370, 374], paragraph 0055);

       if the cryptographic communication channel information is stored, setting key information in the cryptographic communication channel information for the terminal (Figure 5 [blocks 370, 374], paragraph 0055); and,

if the cryptographic communication channel information is not stored, making agreement

on the cryptographic communication channel information, storing the agreed cryptographic

communication channel information in the cryptographic communication channel information

storage part as well as setting the agreed cryptographic communication channel information for

the terminal (paragraph 0043, i.e. using entitlement control messages to update descrambling

keys and access criteria).

36.   Concerning claim 17, Candelore teaches if agreement on cryptographic communication

channel information for the packet is required (Figure 5 [blocks 370, 374], paragraph 0055);

performing the determination about whether valid cryptographic communication channel

information is stored in the cryptographic communication channel information storage part

(Figure 5 [blocks 370, 374], paragraph 0055).

37.   Lee teaches determining first whether address information in the received packet is stored

in a filter information storage part (Figure 2 [block 130], paragraph 0051).

38.   Regarding claim 18, Candelore teaches a readable recording medium on which a program

for causing a computer to perform the packet cryptographic processing method according to any

of one Claims 13 to 17 is recorded (paragraph 0065).

Conclusion

39.   The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure.

40.   The following patents are cited to further show the state of the art with respect to

accessing a third party through a gateway, such as:

        United States Patent No. 7,181,612 B1 to Pellacuru et al., which is cited to show

facilitating IPSec through a Network Address Translation gateway.

        United States Patent No. 6,081,900 A to Subramaniam et al., which is cited to show

accessing a secure server through a secure gateway.

41.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

42.   A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing

date of this final action.

43.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Christian LaForgia whose telephone number is (571)272-3792.

The examiner can normally be reached on Monday thru Thursday 7-5.

44.   If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kristine L. Kincaid can be reached on (571) 272-4063. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

45.   Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2139

clf